Congruences and exponential sums over multiplicative subgroups in finite fields

Iurii Shteinikov (on a joint work with B. Murphy, M. Rudnev and I. Shkredov)

SRISA

Analysis Mathematica Conference 2019

Beginning

Gauss sums are the following quantities $S_n(a, p)$

$$S_n(a, p) = \sum_{0 \le x \le p-1} \exp\{2\pi i \frac{ax^n}{p}\}.$$

Let G be multiplicative subgroup of the field with p elements

Let $S(a, G)$ be the following expression
$S(a, G) = \sum_{g \in G} \exp\{2\pi i \frac{ag}{p}\}.$

Beginning

Gauss sums are the following quantities $S_n(a,p)$

$$S_n(a,p) = \sum_{0 \le x \le p-1} \exp\{2\pi i \frac{ax^n}{p}\}.$$

Let G be multiplicative subgroup of the field with p elements

Let $S(a,G)$ be the following expression
$S(a,G) = \sum_{g \in G} \exp\{2\pi i \frac{ag}{p}\}$.

History

If $G-$ is a subroup of quadratic residues, the following sums can be found

$$S_{2,p}(a) = i^{(\frac{p-1}{2})^2} \left(\frac{a}{p}\right)\sqrt{p}.$$

In general case we have an estimate

$$|S(a,G)| < \sqrt{p}.$$

There is a question for the upper nontrivial estimates for $|S(a,G)|$ where $|G| \leq \sqrt{p}$.

History

If $G-$ is a subroup of quadratic residues, the following sums can be found

$$S_{2,p}(a) = i^{(\frac{p-1}{2})^2} \left(\frac{a}{p}\right)\sqrt{p}.$$

In general case we have an estimate

$$|S(a,G)| < \sqrt{p}.$$

There is a question for the upper nontrivial estimates for $|S(a,G)|$ where $|G| \leq \sqrt{p}$.

History

If $G-$ is a subroup of quadratic residues, the following sums can be found

$$S_{2,p}(a) = i^{(\frac{p-1}{2})^2} \left(\frac{a}{p} \right) \sqrt{p}.$$

In general case we have an estimate

$$|S(a, G)| < \sqrt{p}.$$

There is a question for the upper nontrivial estimates for $|S(a, G)|$ where $|G| \leq \sqrt{p}$.

Applications of $S(a, G)$

Pseudorandom sequences;

Special equations, number of solutions;

Fermat quotients;

Distribution of elements of multiplicative subgroups.

For integer $m \geq 1$ let $T_m(G)$ be the number of solutions of the following equation

$$x_1 + \ldots + x_m = y_1 + \ldots + y_m \pmod p, x_i, y_j \in G.$$

Upper estimates for $|S(a, G)|$ can be obtained from the following inequality

Теорема

For any positive integers m, l we have :

$$|S(a, G)| \leq (pT_l(G)T_m(G))^{\frac{1}{2lm}} |G|^{1-\frac{1}{l}-\frac{1}{m}}.$$

For integer $m \geq 1$ let $T_m(G)$ be the number of solutions of the following equation

$$x_1 + \ldots + x_m = y_1 + \ldots + y_m \pmod p, x_i, y_j \in G.$$

Upper estimates for $|S(a, G)|$ can be obtained from the following inequality

Теорема

For any positive integers m, l we have :

$$|S(a, G)| \leq (pT_l(G)T_m(G))^{\frac{1}{2lm}}|G|^{1-\frac{1}{l}-\frac{1}{m}}.$$

Estimates for T_k

D.R. Heath-Brown and и S.V. Konyagin proved the following result, based on S.A. Stepanov's method, (the case $m = 2$); later S.V. Konyagin obtained for all $m > 2$.

Теорема

For any integer m there is $C(m)$, such that for all p, G, with $t = |G| < p^{2/3}$, $m = 2$ or $t = |G| < p^{1/2}$, $m > 2$, we have

$$T_m(G) \le C(m) t^{2m-2+\frac{1}{2^{m-1}}}.$$

It allowed to deduce the following result.

Теорема

There exists the function $C(\varepsilon) > 0$, such that if $|G| > p^{1/4+\varepsilon}$, then we have

$$|S(a, G)| = O(|G| p^{-C(\varepsilon)}).$$

Estimates for T_k

D.R. Heath-Brown and и S.V. Konyagin proved the following result, based on S.A. Stepanov's method, (the case $m = 2$); later S.V. Konyagin obtained for all $m > 2$.

Теорема

For any integer m there is $C(m)$, such that for all p, G, with $t = |G| < p^{2/3}$, $m = 2$ or $t = |G| < p^{1/2}$, $m > 2$, we have

$$T_m(G) \leq C(m) t^{2m-2+\frac{1}{2^{m-1}}}.$$

It allowed to deduce the following result.

Теорема

There exists the function $C(\varepsilon) > 0$, such that if $|G| > p^{1/4+\varepsilon}$, then we have

$$|S(a, G)| = O(|G| p^{-C(\varepsilon)}).$$

Next progress

Yu. Malykhin obtained nontrivial estimates for T_k and $S(a, G)$ in the case $G \subseteq (\mathbb{Z}/p^2\mathbb{Z})^*$ and proposed a method for such estimates in $\mathbb{Z}/p^k\mathbb{Z}$.

J.Borgain and S.V. Konyagin obtained the following result with combinatorial arguments

Теорема

There exists a function $C(\varepsilon) > 0$, such that if $|G| > p^{\varepsilon}$, then we have

$$|S(a, G)| = O(|G|p^{-C(\varepsilon)}).$$

J. Bourgain obtained such result for all composite numbers q

Next progress

Yu. Malykhin obtained nontrivial estimates for T_k and $S(a, G)$ in the case $G \subseteq (\mathbb{Z}/p^2\mathbb{Z})^*$ and proposed a method for such estimates in $\mathbb{Z}/p^k\mathbb{Z}$.
J.Borgain and S.V. Konyagin obtained the following result with combinatorial arguments

Теорема

There exists a function $C(\varepsilon) > 0$, such that if $|G| > p^{\varepsilon}$, then we have

$$|S(a, G)| = O(|G|p^{-C(\varepsilon)}).$$

J. Bourgain obtained such result for all composite numbers q

Next progress

Yu. Malykhin obtained nontrivial estimates for T_k and $S(a, G)$ in the case $G \subseteq (\mathbb{Z}/p^2\mathbb{Z})^*$ and proposed a method for such estimates in $\mathbb{Z}/p^k\mathbb{Z}$.
J.Borgain and S.V. Konyagin obtained the following result with combinatorial arguments

Теорема

There exists a function $C(\varepsilon) > 0$, such that if $|G| > p^\varepsilon$, then we have

$$|S(a, G)| = O(|G| p^{-C(\varepsilon)}).$$

J. Bourgain obtained such result for all composite numbers q

Теорема

(I. Shkredov, 2014) If $t = |G| \leq \sqrt{p}$ then we have

$$T_2(G) = O(t^{2\frac{1}{2} - C(\alpha)} (\log t)^C),$$

where $C-$ is some positive function and $t = p^\alpha$.

Теорема

(I.S, 2015) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^{4\frac{3}{14}} (\log t)^C),$$

where $C-$ is some absolute constant.

Теорема

(B. Murphy, M. Rudnev, I. Shkredov, Yu. Sh., 2017) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^4 \log t).$$

Теорема

(I. Shkredov, 2014) If $t = |G| \leq \sqrt{p}$ then we have

$$T_2(G) = O(t^{2\frac{1}{2} - C(\alpha)} (\log t)^C),$$

where $C-$ is some positive function and $t = p^{\alpha}$.

Теорема

(I.S, 2015) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^{4\frac{3}{14}} (\log t)^C),$$

where $C-$ is some absolute constant.

Теорема

(B. Murphy, M. Rudnev, I. Shkredov, Yu. Sh., 2017) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^4 \log t).$$

Теорема

(I. Shkredov, 2014) If $t = |G| \leq \sqrt{p}$ then we have

$$T_2(G) = O(t^{2\frac{1}{2} - C(\alpha)} (\log t)^C),$$

where $C-$ is some positive function and $t = p^{\alpha}$.

Теорема

(I.S, 2015) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^{4\frac{3}{14}} (\log t)^C),$$

where $C-$ is some absolute constant.

Теорема

(B. Murphy, M. Rudnev, I. Shkredov, Yu. Sh., 2017) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^4 \log t).$$

Elements of the proof

Denote the quantity
$r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.
We see that

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv) \in G^4$.
This is a surjective homomorphism which kernel consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where
$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

Denote the quantity
$r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.
We see that

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv) \in G^4$.
This is a surjective homomorphism which kernel consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where
$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

Denote the quantity
$r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.
We see that

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv) \in G^4$.
This is a surjective homomorphism which kernel consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where
$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

Denote the quantity
$r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.
We see that

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv) \in G^4$.
This is a surjective homomorphism which kernel consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where
$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2} \sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a+wz))^2.$$

Using standart inequality and we have to deal with the sum

$$\sum_{z,w} \sum_a r^2_{(G-w)(G-z)}(a+wz).$$

This is the number of solutions of the equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ belongs to one line.
and we have to estimate the number of collinear triples
From the results of S.V. Konyagin (or D.A. Mitkin) this quantity is easily estimated.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2}\sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a+wz))^2.$$

Using standart inequality and we have to deal with the sum

$$\sum_{z,w}\sum_a r^2_{(G-w)(G-z)}(a+wz).$$

This is the number of solutions of the equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ belongs to one line.
and we have to estimate the number of collinear triples
From the results of S.V. Konyagin (or D.A. Mitkin) this quantity is easily estimated.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2} \sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a+wz))^2.$$

Using standart inequality and we have to deal with the sum

$$\sum_{z,w} \sum_a r^2_{(G-w)(G-z)}(a+wz).$$

This is the number of solutions of the equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ belongs to one line.
and we have to estimate the number of collinear triples
From the results of S.V. Konyagin (or D.A. Mitkin) this quantity is easily estimated.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2}\sum_a\left(\sum_{z,w} r_{(G-w)(G-z)}(a+wz)\right)^2.$$

Using standart inequality and we have to deal with the sum

$$\sum_{z,w}\sum_a r^2_{(G-w)(G-z)}(a+wz).$$

This is the number of solutions of the equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ belongs to one line.
and we have to estimate the number of collinear triples
From the results of S.V. Konyagin (or D.A. Mitkin) this quantity is easily estimated.

Thank you for your attention